

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-44642

(43) 公開日 平成8年(1996)2月16日

(51) Int.Cl.⁶

G 0 6 F 13/00

識別記号

3 5 1 M 7368-5E

3 5 3 T 7368-5E

3 5 5 7368-5E

9466-5K

F I

技術表示箇所

H 0 4 L 12/56

H 0 4 L 11/ 20

1 0 2 A

審査請求 未請求 請求項の数21 F D (全 18 頁)

(21) 出願番号 特願平6-333261

(22) 出願日 平成6年(1994)12月15日

(31) 優先権主張番号 1 6 8 0 4 1

(32) 優先日 1993年12月15日

(33) 優先権主張国 米国 (US)

(71) 出願人 595008191

チェックポイント、ソフトウェア、テクノロジー、リミテッド

CHECKPOINT SOFTWARE TECHNOLOGIES, LTD.

イスラエル国ラマト-ガン、アバ、ヒレル、シルバー、ロード、7、シルバー、ハウス

(72) 発明者 ギル、シウェド

イスラエル国エルサレム、ピライク、ストリート、6

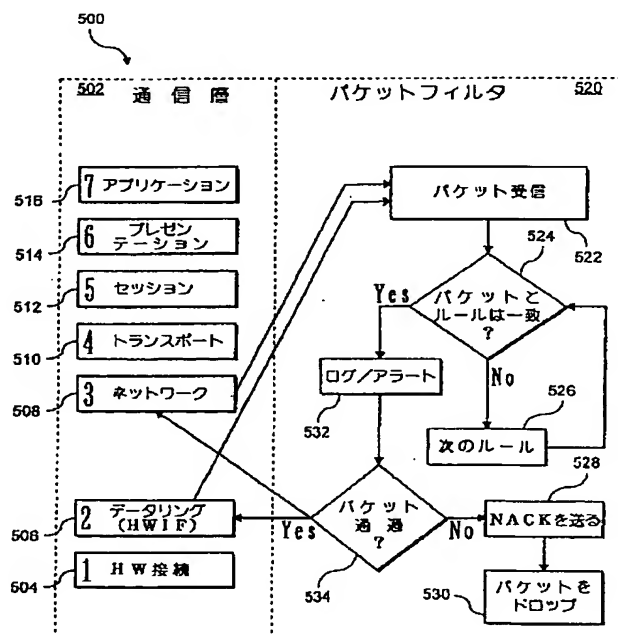
(74) 代理人 弁理士 佐藤 一雄 (外3名)

(54) 【発明の名称】 コンピュータネットワークの制御方法及び保安システム

(57) 【要約】

【目的】 コンピュータネットワーク上の情報の流れを制御する、フレキシブルで容易に変更可能な保安方法の提供。

【構成】 フィルタモジュールがネットワーク内のトラヒックについての保安ルールを特定しそしてこの保安ルールに従って通信パケットを受け入れまたは落とすことによりネットワークの安全性を制御する。一群の保安ルールがハイレベル形式で定義されそしてパケットフィルタコードに変換される。このパケットフィルタコードはネットワーク内の戦略的な点に置かれたパケットフィルタモジュールにロードされる。これら位置に送られまたは入る各パケットはパケットフィルタコード内の命令を実行することで検査される。パケットフィルタコード演算の結果がパケットを受け入れる (パス) か排除 (ドロップ) して通信の試みを不能とするかを決定する。



【特許請求の範囲】

【請求項 1】データがデータパケットとして扱われるコンピュータネットワークにおける上記データパケットの伝送を保安ルールに従って制御するための、下記段階を含む方法：

- a) 保安ルールにより制御される上記ネットワークの夫々のアスペクトの定義を発生する段階；
- b) 上記アスペクトの内の少くとも一つを制御するために上記アスペクト定義で上記保安ルールを発生する段階；
- c) 上記データパケットの伝送を制御するパケットフィルタリングモジュールの動作を制御するために上記保安ルールを一セットのフィルタ言語命令に変換する段階；
- d) 上記ルールに従って上記データパケットの伝送を制御するために、パケットフィルタリング仮想計算機をつくるパケットフィルタモジュールを少くとも一つのネットワークエンティティに設ける段階；
- e) 上記ネットワーク内の上記パケットの伝送を許可または拒否するために上記パケットフィルタリングモジュール仮想計算機を動作させるために上記モジュールが上記命令を読み取りそして実行する段階。

【請求項 2】前記アスペクトはネットワークオブジェクトを含む請求項 1 の方法。

【請求項 3】前記アスペクトはネットワークサービスを含む請求項 1 の方法。

【請求項 4】前記アスペクトはネットワークサービスを含む請求項 2 の方法。

【請求項 5】前記オブジェクト定義は前記オブジェクトのアドレスを含む請求項 4 の方法。

【請求項 6】前記段階 c) のフィルタ言語命令はスクリプトの形であり、更にこのスクリプトを前記段階 e) で実行される前記命令にコンパイルするためのコンパイラを含む請求項 1 の方法。

【請求項 7】前記段階 a) および b) において、前記ネットワークのアスペクトおよび前記保安ルールのアスペクトが図形的に定義されるごとくになった請求項 1 の方法。

【請求項 8】データがデータパケットとして伝送されるコンピュータネットワーク用の保安システムであって、保安ルールに従って上記ネットワーク内の上記データパケットの伝送を制御し、この保安ルールにより制御される上記ネットワークの各アスペクトをこの保安ルールがそれらアスペクトで定義しそしてフィルタ言語命令に変換するようになった保安システムにおいて、下記段階を含む上記システムを動作させる方法：

- a) 上記保安ルールにより制御されるべき上記ネットワークの少くとも 1 つのエンティティに、上記データパケットの伝送を制御するパケットフィルタリング仮想計算機をつくるパケットフィルタモジュールを設ける段階；
- b) 上記ネットワーク内の上記パケットの伝送を許可し

または拒否するために上記パケットフィルタリングモジュールを動作させるために、上記モジュールが上記命令を読み取りそして実行する段階。

【請求項 9】前記アスペクトはネットワークオブジェクトを含む請求項 8 の方法。

【請求項 10】前記アスペクトはネットワークサービスを含む請求項 8 の方法。

【請求項 11】前記アスペクトはネットワークサービスを含む請求項 9 の方法。

10 【請求項 12】前記オブジェクト定義は前記オブジェクトのアドレスを含む請求項 11 の方法。

【請求項 13】前記仮想計算機はデータ抽出動作を行うごとくになった請求項 8 の方法。

【請求項 14】前記仮想計算機は論理動作を行うごとくになった請求項 13 の方法。

【請求項 15】前記仮想計算機は比較動作を行うごとくになった請求項 14 の方法。

【請求項 16】データがデータパケットとして伝送されるコンピュータネットワーク用の保安システムであって、保安ルールに従って上記ネットワーク内の上記データパケットの伝送を制御し、この保安ルールにより制御される上記ネットワークの各アスペクトをこの保安ルールがそれらアスペクトで定義しそしてフィルタ言語命令に変換するようになった保安システムであって、下記段階を含む上記システムを動作させる方法：

- a) 上記保安ルールにより制御されるべき上記ネットワークの少くとも 1 つのエンティティに、上記データパケットの伝送を制御するパケットフィルタリングモジュールをエミュレートするパケットフィルタモジュールを設ける段階；
 - b) パケットフィルタリング動作に上記モジュールが命令を読み取りそして実行する段階；
 - c) 上記段階 b) の結果を記憶装置に記憶する段階；
 - d) 上記ネットワーク内の上記パケットの伝送を許可しまたは拒否するために上記パケットフィルタモジュールを動作させるために、上記命令を上記モジュールが読取って実行しそして上記記憶された結果を利用する段階。
- 【請求項 17】前記アスペクトはネットワークオブジェクトを含む請求項 16 の方法。
- 40 【請求項 18】前記アスペクトはネットワークサービスを含む請求項 16 の方法。
- 【請求項 19】前記アスペクトはネットワークサービスを含む請求項 17 の方法。
- 【請求項 20】前記オブジェクト定義は前記オブジェクトのアドレスを含む請求項 19 の方法。
- 【請求項 21】データがデータパケットとして伝送されるコンピュータネットワーク用の保安システムであって、保安ルールに従って上記ネットワーク内の上記データパケットの伝送を制御し、この保安ルールにより制御される上記ネットワークの各アスペクトを定義しそして

3

フィルタ言語命令に変換するようになった保安システムにおいて、下記要件を含む保安装置：

- a) 上記保安ルールにより制御されるべき上記ネットワークの少なくとも 1 個のエンティティに、上記データパケットの伝送を制御するパケットフィルタリング仮想計算機をつくるパケットフィルタモジュールを設ける手段；
- b) 上記モジュール内にあって、上記ネットワーク内の上記パケットの伝送を許可または拒否するために上記パケットフィルタリングモジュールを動作させるために、上記命令を読み取りそして実行するための手段。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は一般にコンピュータネットワークの安全性を制御する方法に関し、詳細には外部および内部の宛先に対するネットワーク上の情報の流れを制御するコンピュータネットワークの保安のための容易に変更可能なまたは拡張可能な方法に関する。

【0002】

【従来の技術】 殆どの組織の計算環境において、接続性と保安性は二つの矛盾する対象物である。典型的な現代の計算システムは多数のサービスに対して即応型のアクセスを与えるネットワーク通信に関してつくられる。これらサービスの大域的な使用の可能性はおそらく現代の計算の解の唯一最重要な特徴である。接続性の要求は組織内からそしてその外側からも入る。

【0003】

【発明が解決しようとする課題】 許可のない使用についてネットワークサービスを保護することはいずれの組織にとっても重要なことである。例えば UNIX ワークステーションは一旦インターネットに接続されると全世界に、次のテーブル上の他のステーションにそれが提供するサービスのすべてを提供することになる。現在の技術を用いれば、一つの組織は、外部世界または他のサイトへのすべての接続を解消する程度にさえ弱点の防止のためにその接続性の殆どを放棄しなければならない。

【0004】 保安要求の増大に伴い、ネットワーク資源へのアクセスを制御するための手段が管理上で優先的なものとなっている。コストを節約し製造性を維持するために、アクセス制御はその構成が単純であり、ユーザおよびアプリケーションに対し透明でなくてはならない。機械設備のコストの低減とダウン時間の短縮も重要な因子である。

【0005】 パケットフィルタリングはトラフィックを制御することにより、保安性を与えつつ接続性を可能にして、単一ネットワーク内および接続ネットワーク間の不法な通信の試みを防止する一つの方法である。

【0006】 パケットフィルタリングの現在の実行は固定フォーマットに従ってのアクセスリストテーブルの仕様を可能にする。この方法は与えられた組織の保安ポリシーを表わすについてのそのフレキシビリティに限界が

4

ある。またこれは特定のテーブル内に限定されたプロトコルおよびサービス群に制限される。この方法は元のテーブルに特定されていない、異なるプロトコルまたはサービスの導入を許さない。

【0007】 パケットフィルタリングを実行するための他の方法は組織内の戦略的なポイント毎にコンピュータオペレーティングシステムコートを手動的に調整するものである。この方法はネットワークボロジーの将来の変更、新しいプロトコル、向上したサービス、およびそこでこの将来の保安性に対するそのフレキシビリティに境界がある。これは所有するコンピュータプログラムの変更によりエキスパートによる多量のワークを必要とし、その構成と維持を不充分且つ安価なものにする。

【0008】 本発明の目的はコンピュータネットワーク上の情報の流れを制御する、フレキシブルで容易に変更可能な保安方法を提供することである。

【0009】 本発明の他の目的は内部並びに外部の宛先についてネットワーク上の情報の流れを制御する方法を提供することである。

【0010】 本発明の更に他の目的はパケットを許可（パス）または拒否（ドロップ）するために一つのノードの与えられた保安ポリシーを実行するために一組の命令により制御される一般的なパケットフィルタモジュールを提供することである。

【0011】 更に他の目的はパケットフィルタ自体の性質を変える必要なくあるいは長いコードを書込む必要なしにシステム管理プログラムにより容易に変更しうる、コンピュータネットワーク用の保安方法を提供することである。

【0012】

【課題を解決するための手段】 これらおよび他の目的、特徴および利点は、データがデータパケットとして伝送されるコンピュータネットワークを動作させるための、保安ルールに従ってそのネットワーク内のデータパケットの流れを制御するための方法であって、保安ルールにより制御されるネットワークの夫々のアスペクトの定義を発生する段階、上記アスペクトの内の少なくとも一つを制御するために上記アスペクト定義で上記保安ルールを発生する段階、上記データパケットの流れを制御するパケットフィルタリングモジュールの動作を制御するために上記保安ルールを一セットのフィルタ言語命令に変換する段階、上記ルールに従って上記データパケットの流れを制御するために、パケットフィルタリング仮想計算機をつくるパケットフィルタモジュールを少なくとも一つのネットワークエンティティに設ける段階、上記ネットワーク内の上記パケットの流れを許可または拒否するために上記パケットフィルタリングモジュール仮想計算機を動作させるために上記モジュールが上記命令を読み取って実行する段階、を含む方法により与えられる。

【0013】 本発明の他の観点はデータがデータパケッ

トとして伝送されるコンピュータネットワーク用の保安システムであって、保安ルールに従って上記ネットワーク内の上記データパケットの伝送を制御し、この保安ルールにより制御される上記ネットワークの夫々のアスペクトをこの保安ルールがそれらアスペクトで定義し、そしてフィルタ言語命令に変換するようになった保安システムにおいて、上記保安ルールにより制御されるべき上記ネットワークの少くとも一つのエンティティに、上記データパケットの伝送を制御するパケットフィルタリング仮想計算機をつくるパケットフィルタモジュールを設ける段階、上記ネットワーク内の上記パケットの伝送を許可または拒否するために上記パケットフィルタリングモジュールを動作させるために、上記モジュールが上記命令を読み取り実行する段階を含む。

【0014】本発明の更に他の観点はデータがデータパケットとして伝送されるコンピュータネットワーク内の保安システムであって、保安ルールに従って上記ネットワーク内の上記データパケットの伝送を制御し、この保安ルールにより制御される上記ネットワークの夫々のアスペクトをこの保安ルールがそれらアスペクトで定義し、そしてフィルタ言語命令に変換するようになった保安システムにおいて、上記保安ルールにより制御されるべき上記ネットワークの少くとも一つのエンティティに、上記データパケットの伝送を制御するパケットフィルタリングモジュールをエミュレートするパケットフィルタモジュールを設ける段階、パケットフィルタリング動作に上記モジュールが命令を読み取り実行する段階、その結果を記憶装置に記憶する段階および記憶された結果を利用して上記ネットワーク内のパケットの流れを許可または拒否するように上記パケットフィルタモジュールを動作させる段階を含むシステム運用方法を含む。

【0015】

【実施例】図1は一例としてのネットワークトポロジを示す。この例では主サイト100はワークステーション102の形のシステム管理機能を含む。このワークステーション102はワークステーション104、経路指定ルータ110およびゲートウェー106を含むネットワークに接続する。経路指定ルータ110は衛星112およびゲートウェー122を介して遠隔サイトに結合する。ゲートウェー106は経路指定ルータ108を介してインターネットに接続する。遠隔サイト120はワークステーション124を含み、これらワークステーションはネットワークにそしてゲートウェー122を介してインターネットに接続する。図示の構成は例であり、本発明を適用しうるネットワークのタイプを限定するものではない。そのようなネットワークの構成の数は無限であり、それら構成をつくる技術は当業者には周知である。本発明はそれらの構成のいずれについても動作しうる。

【0016】図2は本発明を適用した図1のネットワー

クを示している。図2において、図1と同じ要素には同じ参照数字を付して示してある。図示のように、システム管理部102は制御モジュール210、パケットフィルタ発生器208、表示装置206、記憶媒体212を含む。パケットフィルタ204はシステム管理プログラム、ワークステーション104およびゲートウェー106に設けられる。ゲートウェー106は2個のそのようなフィルタを有し、その一方はそのネットワークへの接続点に、他方は経路指定ルータ108への接続点にある。ルータ108と110は夫々この保安システムにより発生されるが本発明の部分ではないプログラミングスキームテーブルを有している。これらテーブルは当業者には周知のようにルータをプログラムするために現在利用されるテーブルに対応する。

【0017】パケットフィルタ204は遠隔サイト120のゲートウェー122にも設けられる。1個のパケットフィルタは衛星112とゲートウェー122の間に、他のパケットフィルタはインターネットとゲートウェー122の間にそして第三のパケットフィルタはゲートウェーとネットワークの間に設けられる。

【0018】情報は当業者には周知のようにパケットの形でネットワークを流れる。図2のパケットフィルタの位置は、ワークステーション、ルータまたはゲートウェーのようなネットワークの特定のオブジェクトに対するデータの流れが制御されるように選ばれる。このように、夫々のワークステーション104はそれに対する情報流が別々に制御されるように一つのパケットフィルタを有する。しかしながら、遠隔サイト120においては、パケットフィルタはゲートウェー122とネットワークの間の接続部に配置されるから、ワークステーション124に対するデータの流れを個々には制御しない。そのような個々の制御が必要な場合には各ワークステーション124にも配置されることになる。夫々のパケットフィルタは、ネットワークがつくられあるいは保安システムが設置される時点で設置される。しかしながら付加的なパケットフィルタは後に設置しうる。これらパケットフィルタは保護を要するワークステーションまたはゲートウェーのようなホスト装置に設置される。

【0019】各パケットフィルタはシステム管理部102内のパケットフィルタ発生器208により発生された一群の命令にもとづき動作する。これら命令は、パケットの許可または拒否用のパラメータを含むテーブルに対してパケットの内容を単にチェックするのではなく、そのパケットについて複合的動作を行いうるようにする。このように各パケットフィルタは大きなフレキシビリティをもって保安ルールの変更を扱うと共にパケットフィルタ自体の構造を変えることなく複数の保安ルールを扱うことが出来る。

【0020】システム管理部は、モニタ206に表示されそして図3について詳述するように、図形ユーザイ

10

20

30

40

50

ンターフェース (GUI) を介して保安ルールに入る。この情報はパケットフィルタ発生器 208 により処理されそして、その結果のコードが希望の機能を行うようにネットワーク内の適正なパケットフィルタに送られる。制御モジュール 210 はシステム管理部がネットワークの動作に追従しうるようにし、記憶装置 212 はそのネットワークの動作そしてそのネットワークへの不法なエントリの試みをログに維持するために利用される。システムオペレータはそれによりネットワークの動作および保安ルールの成功と失敗についての安全なリポートを与えられる。これにより、保安管理部はそのネットワークの接続性を制限することなくそのネットワークの安全性を維持するために適正である変更を行うことが出来る。

【0021】図 3 は図 2 のコンピュータスクリーン 206 を詳細に示す。このスクリーンは 4 個のウィンドー、すなわち左側の 2 個の小さいウィンドーと右側の 2 個の大きなウィンドー、に分けられる。ネットワークオブジェクトおよびサービスは本発明の保安方法で定義されねばならないネットワークの二つのアスペクトである。ウィンドー 304 はシステムに接続するワークステーション、ゲートウェーおよび他のコンピュータハードウェアのようなネットワークオブジェクトを限定するために用いられる。また例えば、会社の財務部、研究開発部および取締役のような種々のデバイスを群化することも出来る。このようにネットワーク上の個々のコンピュータのみならず、ネットワーク上のコンピュータ群へのデータを適正なパケットフィルタの配置により制御することが出来る。これはシステムオペレータにネットワーク上の通信の管理において大きなフレキシビリティが与えられるようにする。例えば CEO や取締役のような会社の財務主任並びに他の高位の社員が財務部と直接的に通信しうるようにし、他のグループからの通信を排除することが出来る。また、すべてのグループからの電子メールは許すが特定のコンピュータ群に対する他の情報要求を制限することも出来る。これによりシステムオペレータはそのネットワークについて内外の安全性を与えうようになる。このオブジェクト定義はネットワーク上のオブジェクトのアドレス並びにそのオブジェクトがそのネットワークについて内部であるか外部であるかについての名前またはグループ、パケットフィルタがそのオブジェクトに設置されているかどうかについての名前またはグループ、および図形記号を含む。図形記号はルールベース管理部 302 に関連して用いられる。

【0022】同様に、ネットワークサービスはスクリーン上のブロック 306 で定義される。これらネットワークサービスは例えばログイン (login)、ルート、システムログ、テルネット (telnet) を含むことが出来る。各サービスは一般および特殊特性により限定される。一般特性は例えばテルネットについては 23 であるサービス “d p o r t (宛先ポート)” を識別するコードストリ

ングを含む。入力パケット、出力パケットを識別するコードストリングが識別される。特殊特性はサービス名、サービスを与えるために用いられるポート、無接続セッションが非活動のままである時間についてのタイムアウト (秒)、すなわち、そのセッションが完了したとされる前にいずれかの方向にパケット伝送がない時間、を含む。サービス定義の他のエレメントは R P C サービスについてのプログラム番号および U D P のような無接続プロトコルを用いる許可されたサービスについてのアウトバウンド接続を含む。

【0023】ブロック 302 は新しい保安ルールが図形的システムに入りうるようにしそれによりシステム管理部が特定の保安ルールを行うまたは保安ルールを変更するためのコードの書込みをしないですむようにする、ルールベース管理部である。システムに新しいルールを入れるには 4 個のエレメントがあればよい。第 1 エレメントはデータパケットのソースであり、第 3 エレメントはそのパケットの宛先である。第 2 エレメントは関連するサービスのタイプであり、第 4 エレメントは行われるべきアクションである。このアクションはパケットの許可でありその場合パケットはソースから宛先に通され、あるいはパケットの拒否でありその場合にはパケットはソースから宛先に通らない。パケットが拒否された場合、アクションは生ぜずあるいはそのパケットが宛先に通されなかったことを示す否定応答を送ることが出来る。更に、特定されうるもう一つのエレメントはどのオブジェクトについてルールが適用されるのかを特定するルールについての設置位置である (図 2 参照)。設置位置が特定されなければシステムは省略により通信宛先にパケットフィルタモジュールを置く。これらオブジェクトは必ずしも宛先である必要はない。例えば、インターネットから局所ホストに宛てた通信は必ずゲートウェーを通る。それ故、そのゲートウェーがソースでもなく宛先でもない場合であっても、ゲートウェーにルールを適用することが出来る。頭字語 (acronyms) または図形記号を伴うデータを入れることにより、各ルールは高速で入れられそしてこの目的のために新しいコードを書込み、コンパイルしそしてチェックする必要なしに検査される。このように、システム管理部は保安目的についてのコンピュータのプログラミングに際してエキスパートである必要はない。サービスがシステムにすでに入っているサービスの内の一つである限り、システム管理部の機能についてホストとしてサービスするコンピュータはその情報を、後述するように適当なパケットフィルタ用の一群の命令へと処理する。

【0024】ブロック 308 は保安システムの構成と動作を要約するシステムスナップショットである。本発明を実施する必要はない。このシステムスナップショットは図形記号を用いてシステムの要約を表示する。例えば、この要約はホストアイコン、ホスト名、ルールベ

10

20

30

40

50

スを含むファイル名であるルールベース名およびルールベースがホストに設置された日付を含むことが出来る。またこれはホストとの通信があったかどうかを示すホストの状態並びにホストにより検査され、ドロップされそしてログされたパケットの数をも示すことが出来る。

【0025】図4はGUI上の情報を、パケットフィルタ用に利用されるルールを含むフィルタスクリプトに変換するサブシステムのフローチャートである。この実施例においては、フィルタスクリプト発生器の出力は後述のようにそのときパケットフィルタモジュールにより行われるオブジェクトコードにコンパイルされる。

【0026】サブシステム400は402でスタートし、ブロック404に移り、ここでGUIから第1ルールを獲る。第1ルールはスクリーンの第1ラインであって、そこで図3に示すように新しい保安ルールが識別される。次に制御はブロック406に移り、そこでそのルールソースをネットワークオブジェクトに一致させるためのコードが発生される。すなわち、データパケットが出るシステムのオブジェクトの一つを表わすものとしてパケットのソースがソースコードブロックに入れられる。次に制御はブロック408に移り、ネットワークのどのオブジェクトにデータパケットが宛てられるかを示すためのコードが宛先コードブロック内に発生される。次に制御はブロック410に移り、選ばれたルールサー

ビスを一致させるためのコードが発生される。これらルールサービスは予め定義されておりそしてシステム内に記憶されるか、あるいは定義されていなければ、そのサービスを調整する保安ルールがシステムに入れられるときに定義される。次に制御はブロック412に入り、データブロック406、408および410が一致したとき、すなわちチェックの結果が真であるときパケットを許可するためまたは拒否するためのコードが発生される。許可または拒否のためのアクションは保安ルールにおいて選ばれたアクションにもとづく。次に制御は決定ブロック414に入り、システムに他のルールを入れるべきかどうかを決定する。他のルールをシステムに入れるべきでない場合には制御はブロック416に入り、次のルールを得てブロック406にもどり、そのときプロセスがくり返されそしてGUIの次のラインである次の保安ルールが処理される。

【0027】通信プロトコルは階層をなしており、従ってプロトコルスタックとも呼ばれる。ISO (International Standard Organization) は通信プロトコル層の設計用のフレームワークを与える一般モデルを定義している。このモデルは現存する通信プロトコルの機能性を理解するための基本的なリファレンスとして作用している。

ISO MODEL

層	機能	例
7	アプリケーション	Telnet, NFS, Novell NCP
6	プレゼンテーション	XDR
5	セッション	RPC
4	トランスポート	TCP, Novell SPX
3	ネットワーク	IP, Novell IPX
2	データリンク (ハードウェアインターフェース)	ネットワークインターフェースカード
1	フィジカル (ハードウェア接続)	Ethernet, Token Ring, TI

【0028】異なる通信プロトコルはISOモデルの異なるレベルを使用する。或る層内のプロトコルは他の層で使用されるプロトコルには無関係となりうる。これは、保安アクションを行うときの重要な因子である。例えば、アプリケーション (レベル7) は通信の試み (レベル2-3) についてソースコンピュータを識別出来ず、それ故充分な保安性を与えることが出来ない。

【0029】図5はISOモデルにおいていかにして本発明のフィルタパケットモジュールを用いるかを示している。ISOモデルの通信層は図5の左側に502で示してある。レベル1、ブロック504、はネットワークの種々のオブジェクトを接続するために用いられるワイヤでよいネットワークのハードウェア接続である。第2レベル、図5のブロック506、はネットワークの各コ

ンピュータに配置されるネットワークインターフェースハードウェアである。本発明のパケットフィルタモジュールはこのレベルと、ネットワークソフトウェアであるレベル3との間に入る。また、ISOモデルの他のレベルは一つのセグメントから次のセグメントにデータを配布することに関連するレベル4、ブロック510、およびネットワーク上の“セッション”の開閉を同期させるレベル5、ブロック512である。レベル6、ブロック514はネットワーク上の種々のコンピュータ間のデータの変化に関係し、レベル7、ブロック516はアプリケーションプログラムである。

【0030】パケットフィルタモジュールのあるコンピュータに入るパケットはレベル1と2を通り、図5の右側に示すパケットフィルタ520に入る。このパケット

10

20

40

50

はブロック522に入る。ブロック524においてこのパケットは保安ルールと比較され、そしてそのパケットがルールと一致するかどうかについての決定がなされる。このパケットとルールが一致すれば、システム管理部のログに入れられそして、システムに入れるための不法な試みがなされたとすれば、アラートが出される。次に制御はブロック534に入り、保安ルールの要件にもとづきこのパケットを通すかどうかの決定がなされる。パケットを通す決定がなされれば、そのパケットはレベル3、ブロック508に通る。このパケットを通さない決定がなされると、もしこのオプションが選ばれれば否定応答(NACK)がブロック528に送られ、そして制御はブロック530に移り、そのパケットがドロップされる、すなわちその宛先に通されない。同様に、アプリケーションが他の宛先に送られるべきパケットを発生するとすれば、そのパケットはレベル3、ブロック508でISOモデルを出てブロック522に入り、そのパケットが通されるべきときにレベル3、ブロック508ではなくレベル2、ブロック506に通される点を除き同じプロセスにより処理される。レベル2において、パケットはブロック504でレベル1に送られる。このパケットがルールと一致しなければ、次のルールがとり出されてそれと一致するかどうかについて検査される。ソース宛先または特定されるサービスには無関係に任意のパケットを一致させる省略ルールが与えられる。他のルールが一致しないとき、このルールがとり出されてそのパケットをドロップさせる。パケットのドロップはこのような場合にとられる最も安全なステップである。勿論“エンプティールール”をパケットの通過のために書込んでもよい。

【0031】図6において、600は図5のブロック520の詳細を示す。図6における一般的な説明と図7～図10に示すより詳細な説明は用語“パケットフィルタモジュール”を定義するものである。これらの図に示す能力はパケットフィルタモジュールの最少の動作能力である。図11～図15はこのパケットフィルタモジュールに含まれるが用語の最少定義には必要ない付加的特徴を示す。

【0032】パケットフィルタモジュールはここではネットワーク上の一つのコンピュータであるホストコンピュータにある、図6～図10に示すマシンのエミュレーション(emulation)として定義される“仮想計算機”として具体化される。

【0033】仮想計算機は図5のブロック522に対応するブロック602でスタートし、パケットを受信する。制御はブロック604に移り、フィルタ動作がメモリ(図示せず)からの命令から得られる。これらフィルタ動作は図2のパケットフィルタ発生器208により発生されたフィルタ動作である。次に制御はブロック604に入りそこでフィルタ動作が得られそしてブロック6

06に入りメモリ618が初期化される。ブロック608において、第1仮想計算機動作が得られそしてブロック610で行われる。この仮想計算機は中間値の記憶に用いられるスタックまたはレジスタ618のようなメモリ機構を含む。このスタックまたはレジスタの利用は表1に関連して詳述する。次に制御は決定ブロック614に入り、ストップ状態となったかどうか決定される。ストップ状態になっていれば次の決定はそのパケットを許可するか拒否するかであり、その決定はブロック616で行われる。パケットが通されていればそのパケットは図5に示すように進む。パケットが拒否されれば、それはドロップされ、そしてブロック528と530に示すように否定応答が送られる。ブロック614でストップ状態になっていなければ、次の動作はブロック616で得られそしてプロセスはブロック610からくり返される。

【0034】ステップ5、ブロック610、で行われる動作のタイプは図7に示してある。図7において、ブロック610と614は図6に示すものと同じである。接続613は並列に示す3つの動作により割込まれる。ブロック610で行われるべき動作について、制御は適正なブロック702、704または706に入り、タスクを行う。ブロック702において、データ抽出が行われ、ブロック704では論理演算が行われ、ブロック706では比較動作が行われる。図7の右側に示すように、他のブロックは仮想計算機により行うことの出来る動作に並列に加えることが出来る。ブロック702、704、706に示すサブセットは本発明の仮想計算機の重要なエレメントである。これらエレメントは夫々図8、9、10に詳細に示してある。仮想計算機により行うことの出来る動作にオプションとして含めることの出来る付加エレメントは夫々図11～図15に示してある。

【0035】データ抽出ブロック702は図8に詳細に示す。このプロセスはブロック802でスタートし、次にブロック804でパケット806内の特定のアドレスからデータが抽出される。このアドレスはスタックメモリ618または命令コードからとり出される。抽出されるデータの量もこのスタックメモリまたは命令コードにより決定される。抽出されたデータはブロック808でメモリストック810に置かれる。このプロセスはブロック812で終了する。これら図面において、制御の流れは単線矢印で、データの流れは二重線矢印で示す。

【0036】図9は論理演算704を詳細に示す。この演算はブロック902でスタートし、ブロック904でメモリ906から第1値が得られる。ブロック908でそのメモリから第2の値が得られ、そして論理演算がブロック910で行われる。この論理演算が真であればブロック912でメモリ906に1が置かれ、誤であればブロック914でメモリ906に0が置かれる。このブ

13

ロセスはブロック916で終了する。

【0037】仮想計算機に要求される第3であって最後の動作を図10に示す。この比較動作、ブロック706、はブロック1002でスタートし、ブロック1004で第1値がメモリ1006より得られる。次にブロック1008で第2値がメモリ1006より得られる。第1および第2値間の比較がブロック1010で行われる。その結果が真であればブロック1012でメモリ1006に1が置かれ、誤であればブロック1014で0が置かれる。このプロセスはブロック1016で終了する。

【0038】次の動作は図7には示していないが、同図の右側に破線で示すように付加されるものであって、ブロック702、704、706と同様に、すなわち並列に接続される。図11はリテラル値のメモリへのロードを示す。このプロセスはブロック1102でスタートし、次にブロック1106で命令コードからリテラル値が得られる。この値はブロック1108でメモリに置かれそしてこのプロセスはブロック1110で終了する。

【0039】条件付ブランチ動作を図12に示す。このプロセスはブロック1202でスタートし、次にブロック1204で命令コードからとり出されたブランチ条件がチェックされる。このブランチ条件がブロック1210において真であれば、ブロック1208でその値がメモリスタック1206から得られる。ブロック1210の比較結果が真であれば次のステップはNにセットすることであり、このプロセスはブロック1216で終了する。ブロック1210での比較が誤であればブロック1204において制御はブロック1214に入る。

【0040】算術またはビット形の演算を図13に示す。このプロセスはブロック1302でスタートし、次にブロック1304でメモリ1306から第1値が得られる。ブロック1308でメモリ1306から第2値が得られ、そしてブロック1310でメモリから得られたこれら二つの値についての算術またはビット型の演算が行われる。この演算の結果はブロック1312でこのメモリに置かれ、そしてこのプロセスはブロック1314で終了する。

【0041】図14は、データが保安ルールを実行する第1群の命令から第2保安ルールについての第2群の命令に通すべきときに有用なルックアップ動作である。図6のブロック606に示すように、新しい保安ルールが処理されるときにメモリが初期化される。それ故、第1の保安ルールによりメモリに置かれた情報は第2保安ル

14

ールによる使用には供されない。この問題を克服するために、別のメモリ1410が与えられる。これはこの目的に利用されるテーブル1〜3を含む。これらテーブルへのデータエントリは図15に示されており、以下これを説明する。ルックアップ動作は1402でスタートし、次に1404においてメモリ1406から値が得られる。次にブロック1408においてブロック1410のテーブル1〜3から参照されるテーブル内の値をサーチすることによりデータが得られる。次にブロック1412でそのブロックがそのテーブルにあるかどうかの決定がなされる。この決定がYであればブロック1416でメモリ1406に1が置かれ、Nであればブロック1414で0が置かれる。このプロセスはブロック1418で終了する。

【0042】図15において、このプロセスはブロック1502でスタートし、次にブロック1504でメモリ1506から値が得られる。次にブロック1508でメモリ1506からの値がブロック1510のテーブル1〜3内の適当な位置に置かれる。次にブロック1512でテーブルに記憶された値が成功したかどうかの決定がなされる。成功であればブロック1516でメモリ1506に1が置かれ、そうでなければブロック1514で0が置かれる。このプロセスはブロック1518で終了する。

【0043】保安ルールの一例は本発明のパケットフィルタリング方法を用いて行われる。それをシステム内のどのテルネット(Telnet)サービスをも許可しないようにする保安ルールを一例として次に述べる。テルネットはTCPサービスとして定義されそして特定のTCP宛先ポートを有する。これはパケットのバイト位置9にTCPプロトコル値6を有することおよびパケットのバイト位置22に宛先テルネットプロトコル数23を有することで識別される。この値は2バイト値である。これはすべてのテルネット要求パケットにある。

【0044】テーブル1内の第1の動作はパケット位置9からIPプロトコルを抽出し、そしてそれをメモリに置くことである。テーブル1の右側の“メモリ値”の欄に示すように、この値6はスタックの上に置かれる。第2の動作、すなわち、上記した6であるTCPプロトコル(ポート)番号はメモリの第2の位置に置かれる。ステップ3において、このスタックのはじめの2層の値が比較されて正の結果を得る。

【0045】

【表1】

テーブル1
ドロップテルネットプロセス

#	パケットフィルタコード	仮想計算機動作	メモリ値 (スタック順)		
1	push byte [9]	抽出動作: パケット位置9からIPプロトコル番号をメモリに抽出	6		
2	push 6	メモリにリテラル値そう入: TCPプロトコル数をメモリに置く	6	6	
3	eq	比較動作: TCPに対しIPプロトコルを比較し、正值を得る	1		
4	pushs [22]	抽出動作: パケット位置22からTCPプロトコル数をメモリに抽出	1	23	
5	push 23	メモリにリテラル値をそう入: TELNETプロトコル数をメモリに置く	1	23	23
6	eq	比較動作: TELNETに対しTCPプロトコルを比較し、正の結果を得る	1	1	
7	and	論理演算: TCPとTELNETが一致したかどうかプロトコルをチェック	1		
8	btrne drop	条件付ブランチ動作: メモリ値が真ならドロップ状態にブランチする			

スタックの上の2層における値6は削除され、そして正の結果を示す1がスタックのトップに置かれる。ステップ4でパケット位置23についてのTCPプロトコル数が抽出されてスタックの第2層のメモリ位置に置かれる。ステップ5でテルネットプロトコル数であるリテラル値がスタックの第3層のメモリに置かれる。ステップ6でテルネット用のTCPプロトコルを含むメモリ層2と3が期待値と比較されて正の結果を得る。このスタックの第2、3層の値が削除され、正の結果を示す1が置かれる。ステップ7でTCPとテルネットの両方が一致したかどうかを見るために論理演算が行われる。これはAND動作により決定される。この場合、結果は正であり、スタックのはじめの2層の1は削除され、正の結果を示す1が置かれる。ステップ8で条件付ブランチ動作が行われ、メモリ値が真であればこのプログラムがドロップ状態にブランチする。この場合、結果は正であり、プログラムはドロップ状態にブランチし、テルネット要求は通されない。このようにテルネットを落すためのこのルールは行われる。

【0046】本発明の特定の実施例について述べたが、或る種の変更が本発明の範囲内で可能なことは当業者には明らかである。例えば上記ではパケットフィルタ動作はスクリプトとして発生されそして次にオブジェクトコードへとコンパイルされたが、それら命令は直接にオブジェクトコードとして発生されてもよく、あるいはスクリプトをオブジェクトコードにコンパイルする必要を避

けるためにインタープリタを使用してもよいことは当業者には明らかである。また、仮想計算機の動作を等価的に行うことも当業者には明らかである。例えば、比較動作は変数から一つの値を減算し、その結果について等化操作を行うことにより行うことが出来る。

【図面の簡単な説明】

【図1】ネットワークトポロジーの一例である。

【図2】図1のネットワークトポロジーに適用した本発明の保安システムを示す図。

【図3】図2のネットワーク管理部のコンピュータスクリーンを詳細に示す図。

【図4】図形情報をフィルタスクリプトに変換するためのサブシステムのフローチャート。

【図5】本発明を用いるコンピュータネットワークにおける情報の流れを示す図。

【図6】図5のパケットフィルタの動作のフローチャート。

【図7】図6のパケットフィルタの動作のフローチャート。

【図8】図7の仮想計算機動作を示すフローチャート。

【図9】図7の論理演算法のフローチャート。

【図10】図7の比較動作法のフローチャート。

【図11】リテラル値をメモリに入れる方法のフローチャート。

【図12】条件付ブランチ動作のフローチャート。

【図13】算術およびビット型演算のフローチャート。

【図 14】 ルックアップ動作のフローチャート。

【図 15】 レコード動作のフローチャート。

【符号の説明】

100 主サイト

102, 104 ワークステーション

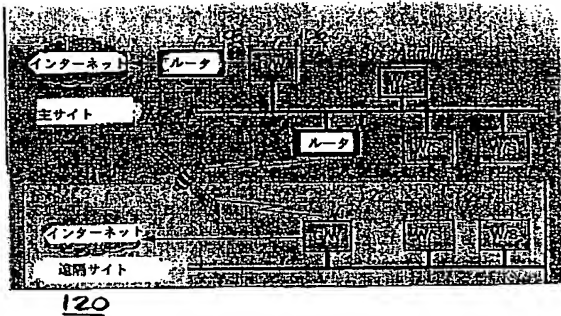
110 ルータ

106 ゲートウェー

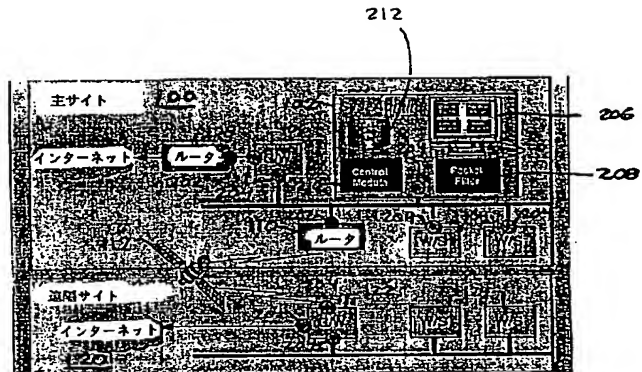
112 衛星

120 遠隔サイト

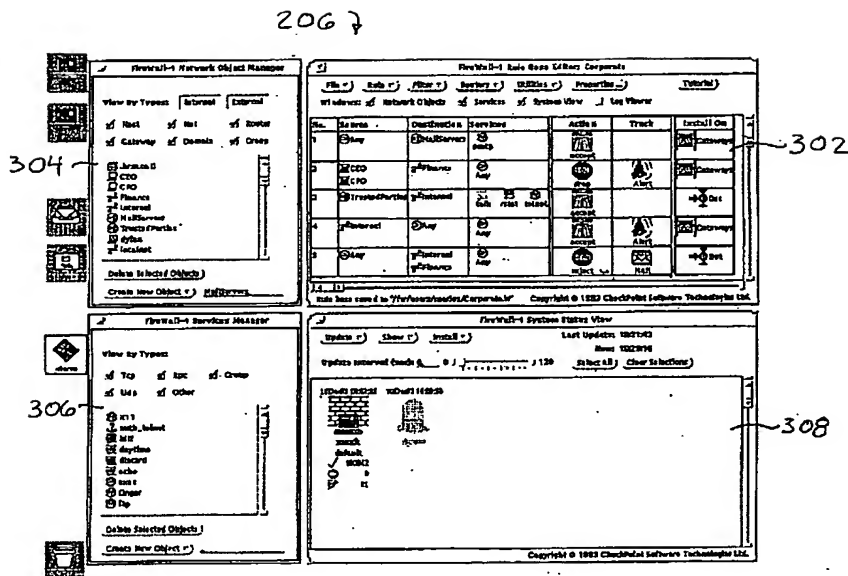
【図 1】



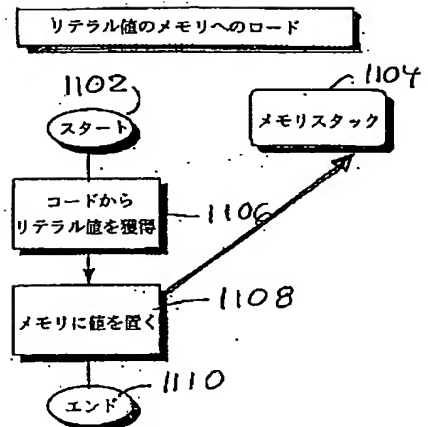
【図 2】



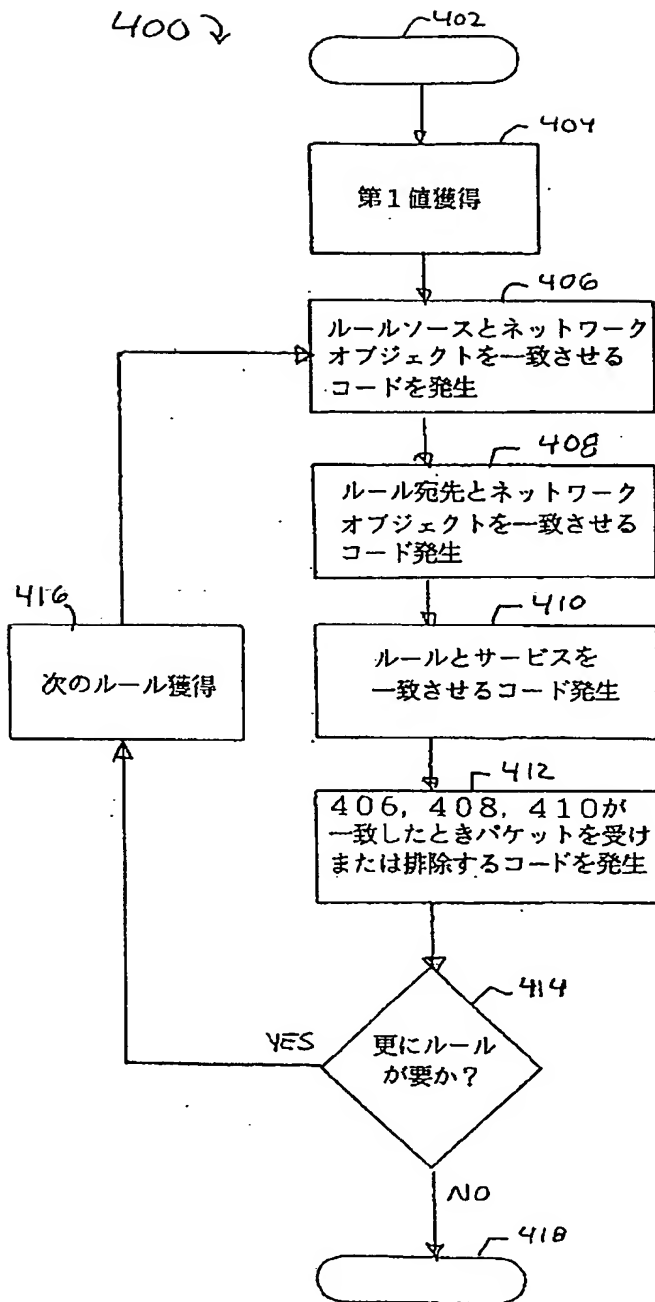
【図 3】



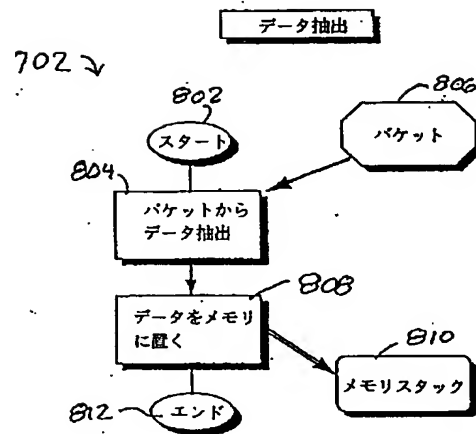
【図 11】



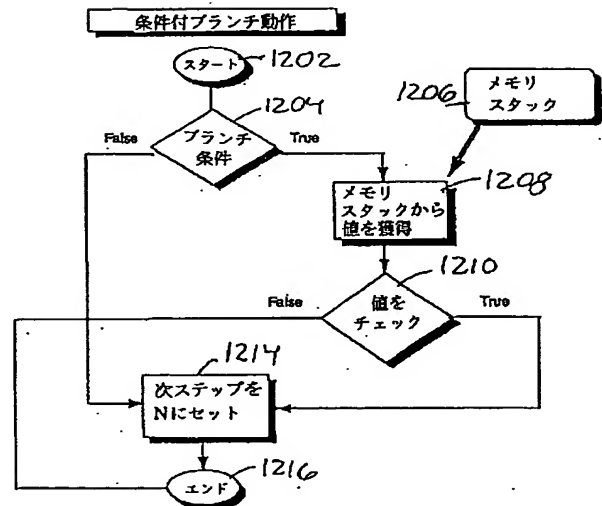
【図 4】



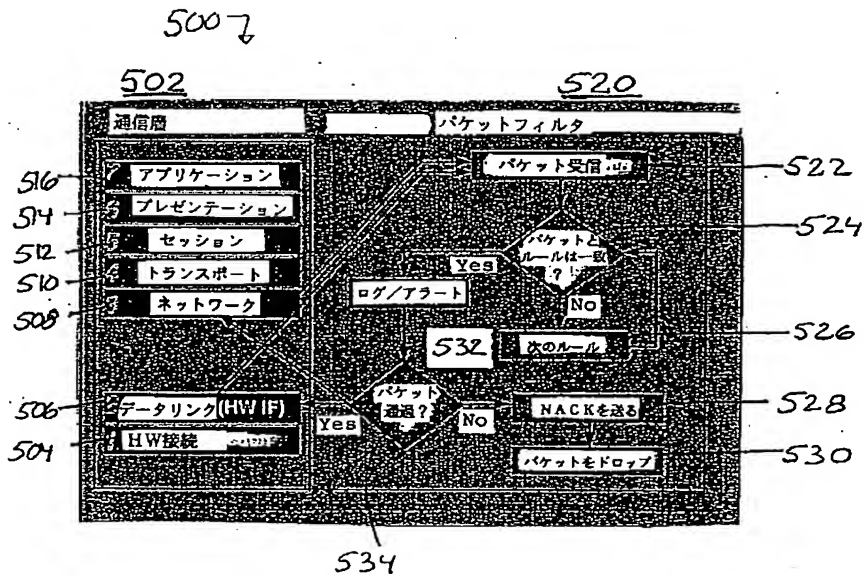
【図 8】



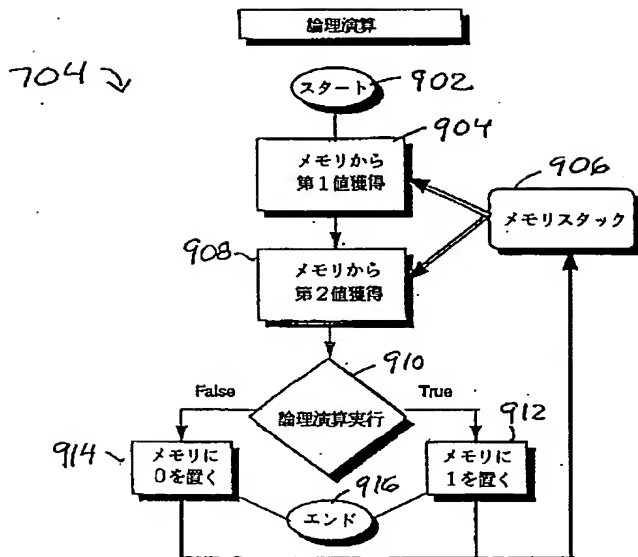
【図 12】



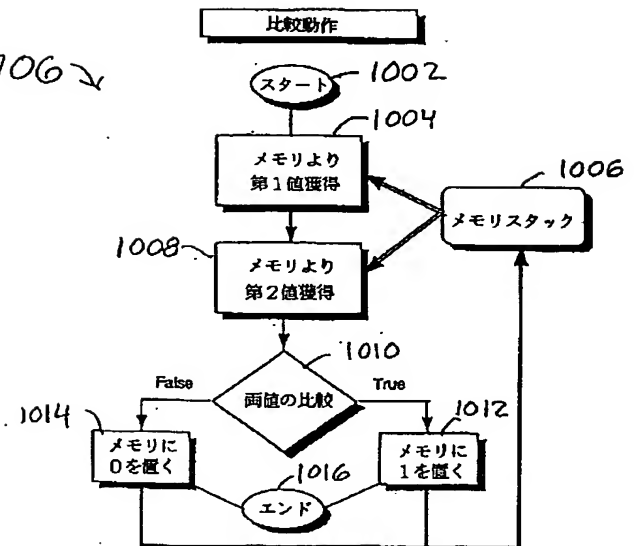
【図5】



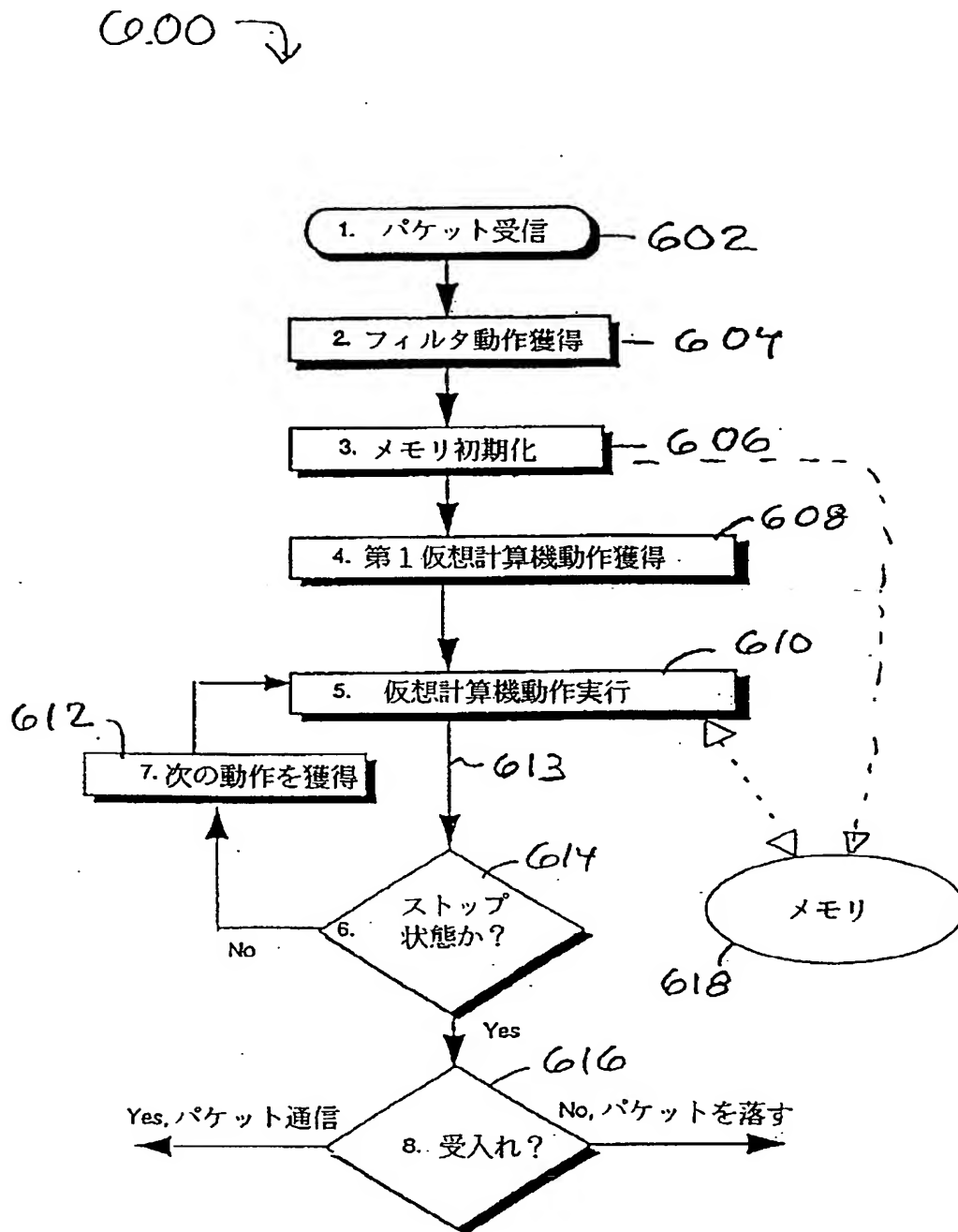
【図9】



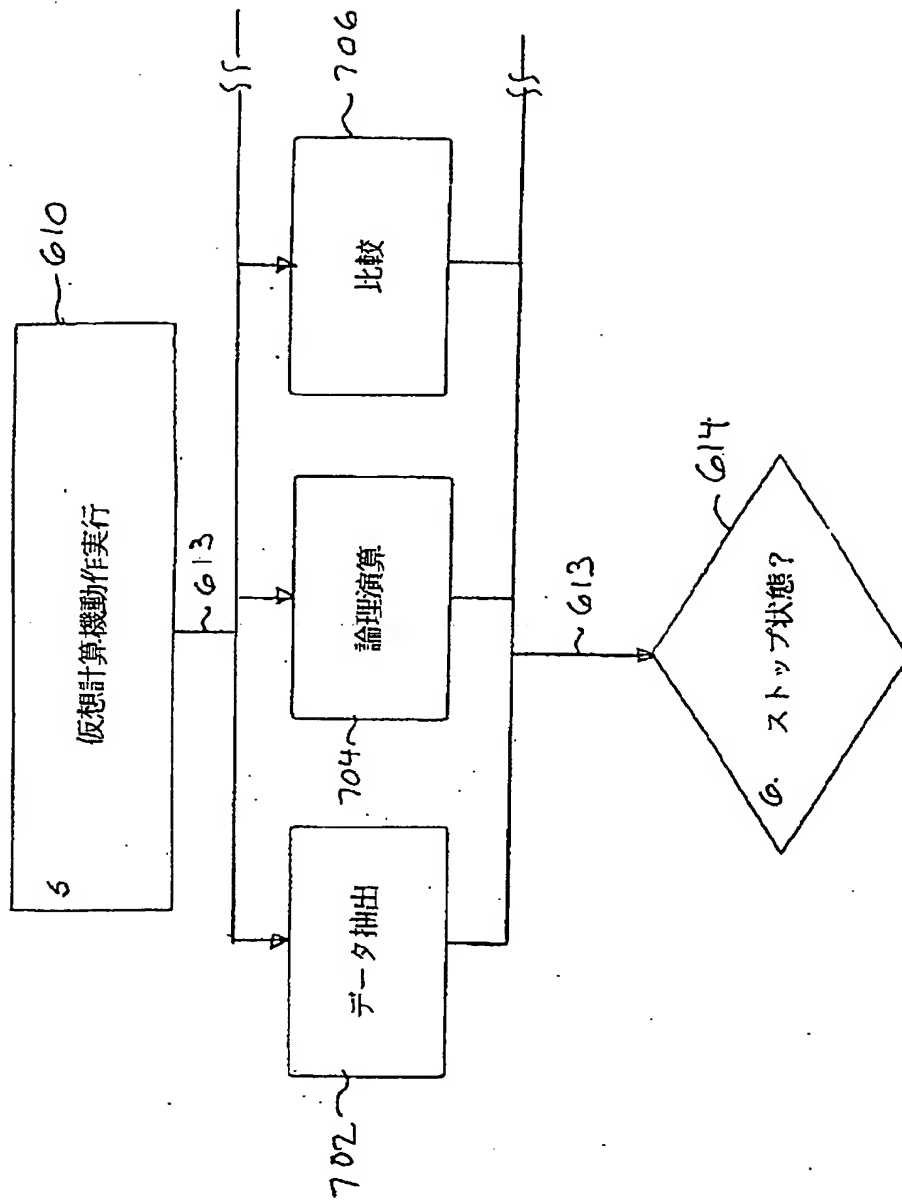
【図10】



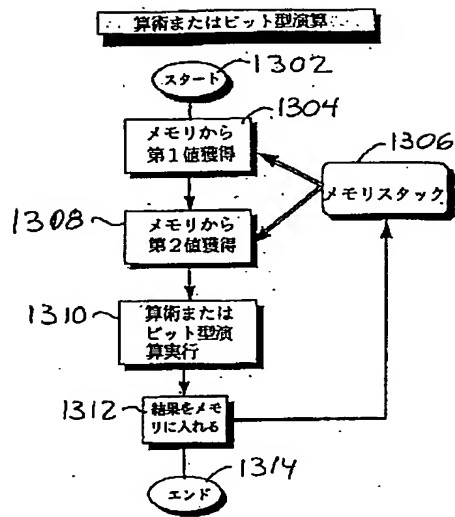
【図 6】



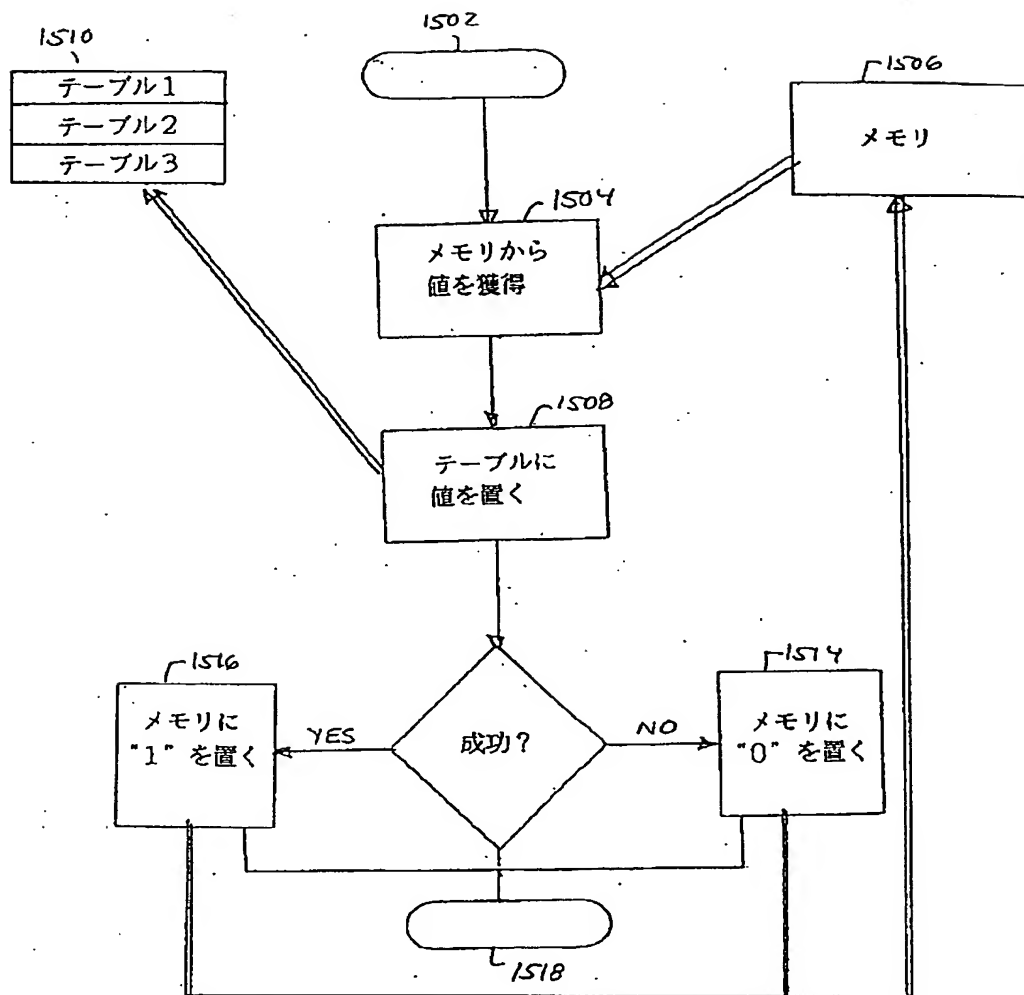
【図 7】



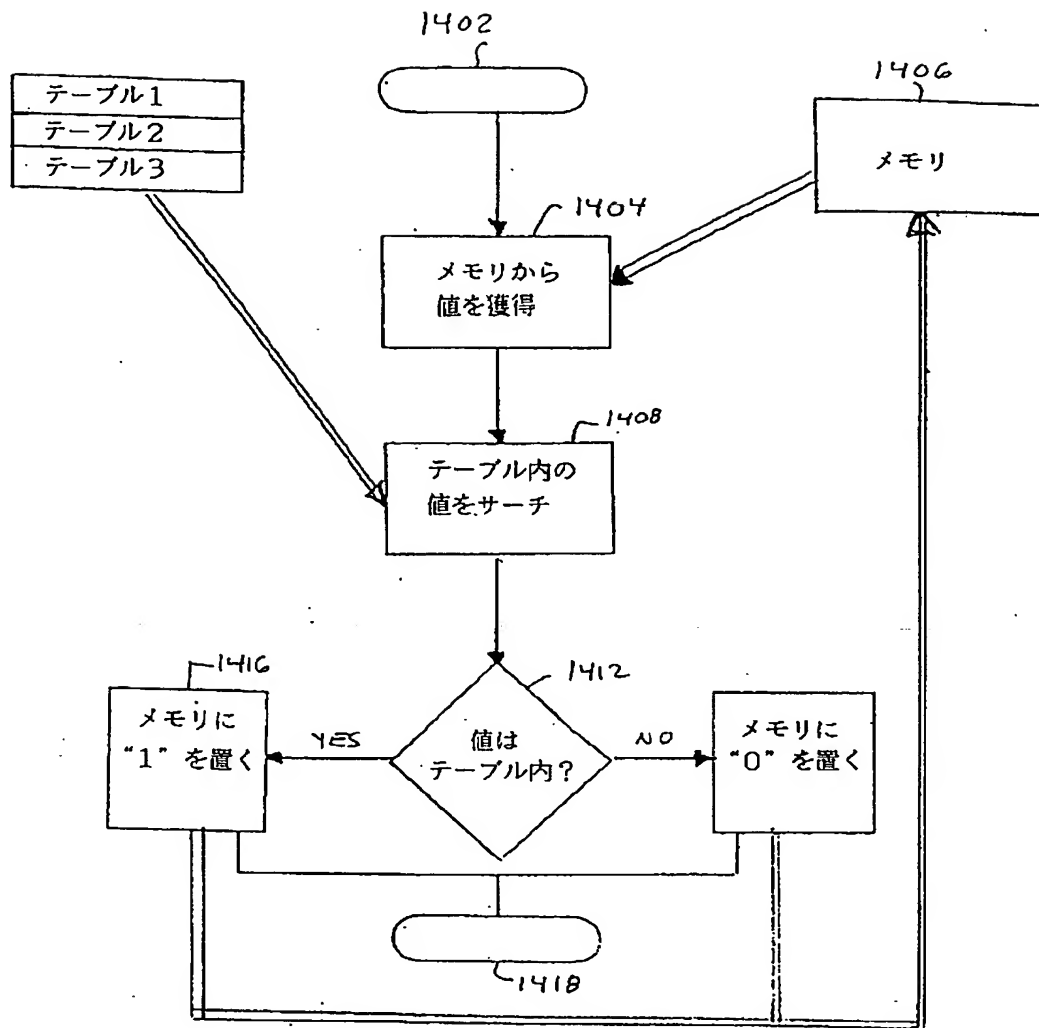
【図13】



【図15】



【図 1 4】



【手続補正書】

【提出日】平成 7 年 5 月 2 日

【手続補正 3】

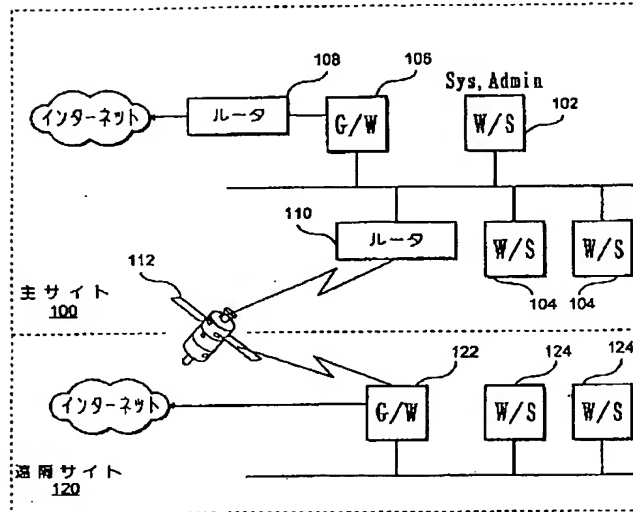
【補正対象書類名】図面

【補正対象項目名】図 1

【補正方法】変更

【補正内容】

【図 1】



【手続補正 4】

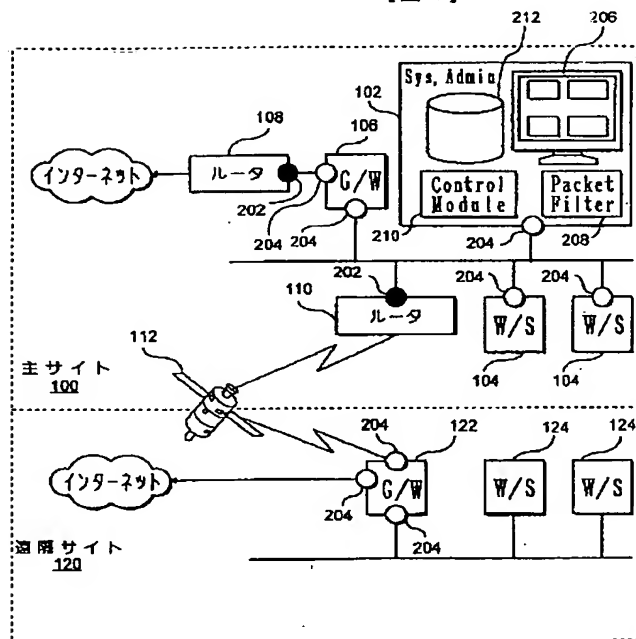
【補正対象書類名】図面

【補正対象項目名】図 2

【補正方法】変更

【補正内容】

【図 2】



【手続補正 5】

【補正対象書類名】図面

【補正対象項目名】図 5

【補正方法】変更

【補正内容】

【図 5】

